Memorandum

Tempe Police Department – Audit and Compliance Unit

TO: Director Brenda Buren, OMBR

FROM: Sergeant Karin Betz, Audit and Compliance Unit

DATE: August 12, 2014

SUBJECT: Automated License Plate Recognition Inspection

Between 8/1/2014 and 8/15/2014 the Audit and Compliance Unit conducted an inspection of the Automated License Plate Recognition (ALPR) program. The ALPR program was transformed within the Tempe Police Department in October 2013 to more fully utilize the technological capabilities of the system. As a result, policy and procedure was updated and a training program was implemented. Inspectors reviewed several areas of the program to ensure compliance with stated policy including:

- Ensure all users of ALPR equipment have completed departmental training.
- Retention of ALPR data is purged form the Department's APLR Server after six months.
- All ALPR queries by law enforcement include a corresponding case number or identification number.

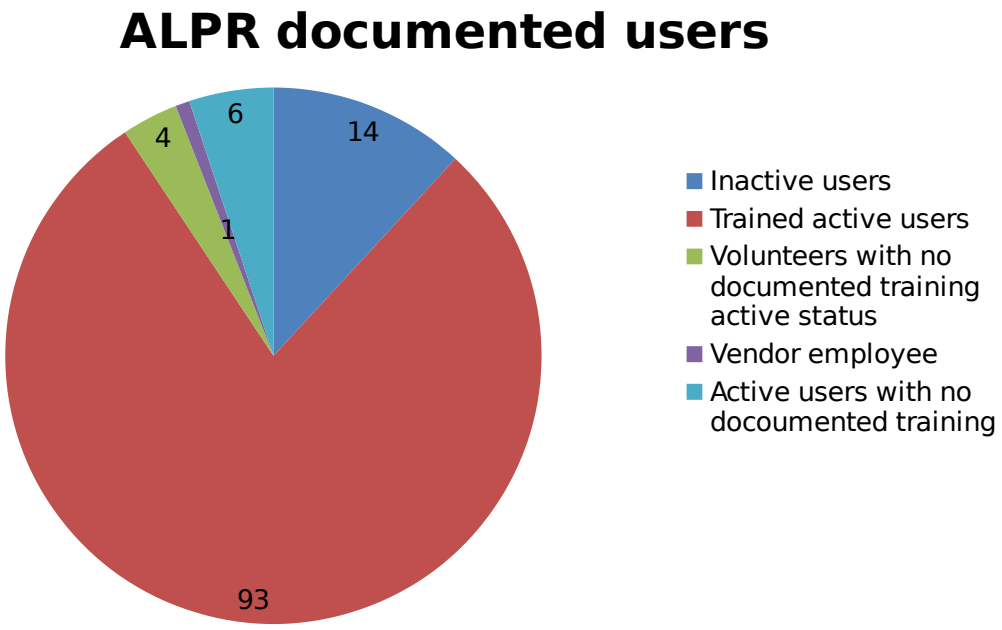
Completion of Departmental Training

According to the ALPR system there are 118 listed users of the system. This includes employees, vendor employees, and Police volunteers with both active and inactive accounts. Inactive accounts were created for employees by the system administrator due to interest expressed in attending a departmental training class, but the employee did not complete the training. Fourteen employees fell into this category.

Initially, sixteen users showed as active users with no documentation of completion of the departmental training. Follow up with ALPR administrators revealed meeting requests or other email communication, as well as independent recollection of the attendance of other active users. Due to the process involved with creating and activating ALPR accounts of trained employees, this documentation was sufficient proof of training and four

additional users were entered into ELM. Another employee was listed as an active user, however, training in ELM was not documented and the ALPR administrator could not recall her attendance in the training. A query revealed no usage of the system by that user. Her status was immediately changed to inactive. One recently retired employee was also still in the system who should have been removed upon separation from employment.

Of the remaining eleven users four users without documentation in ELM are volunteers and one is a vendor employee. The ALPR administrator was not aware volunteers could be added to ELM to document volunteer training. In addition, the training provided to volunteers is modified from the training provided to other users based on the restricted usage of the system by volunteers. Since volunteers do log into the ALPR system and have access, their training should be documented in ELM to comply with current policy. A final count of active users not documented in ELM as having departmental training documented is 11 out of 118 users or approximately 9%.



Retention

The system is set to automatically purge every 180 days. An administrator's account was viewed to confirm the setting of the purge request. In addition, several attempts were made to access data past the 180 day retention period. No data obtained as a result of departmental ALPR equipment was retrievable past a six month time period.

During the course of the audit it was learned some users get automatic emails advising of hits. Theses emails do contain ALPR data. The majority

of the users who receive emails of this nature were contacted to ensure compliance with retention guidelines. Email accounts were viewed to ensure retention guidelines were followed. All users contacted were in compliance with the retention guidelines, most of which did not have data from emails even a week old.

Law enforcement purposes only use

General Order 17.102.D3e states a case number or identification number is required for each system query. The newness of the ALPR program has been taken into account when evaluating this area of the inspection. A pilot group was developed and first trained in October 2013. Other employees began training in January 2014 once the pilot portion of the program concluded.

Records of departmental queries for the time period 5/1/2014-8/6/2014 were obtained and evaluated to ensure compliance. During this time period 667 queries were evaluated for compliance. There were more than 667 queries made by employees during this time, however, only "detection browsing" and "hot plate upload" require the user to enter a report number or identification number. Other types of queries that do not require a report number for viewing are "locate analysis browsing" and "stake out browsing". "Detection report" also does not require a report number, however, in order to obtain a report, a report number needs to be inputted during the "detection browsing" query. The report request is easily tracked by the information inputted on the corresponding "detection browsing" – information that makes up the report. During the course of this inspection the system administrator put forward an inquiry with the vendor to determine if the same audit requirements could be required for all queries.

Of the 667 auditable queries made during this time period, 151 (22.6%) did not have a proper case number submitted with the query. Instead, employees entered generic identifying information such the name of the agency requesting the information, "investigation", "warrant", etc. Although there may be times a query is made that is not tied to a specific incident report, such as if an officer observes a suspicious vehicle and simply queries the plate during a security check while not checking off to create a report number, the majority of queries should and will have a related incident. Warrants queries will also have a related warrant number that can be entered. Requests from officers actively working a legitimate law enforcement investigation may be made through a trained system user who does not have a report number readily available. Often times these requests come from outside agencies who request the information from an intelligence partnership. Since data obtained from these requests are shared with other agencies, confirmation was made that the requestor was able to relate all requests to a particular detective and case. In order to easily track requests in the audit field it was determined that in the future the agency

and requestor would be documented in one audit box, followed by incident number and type of incident in the second audit box. If the request is urgent and the incident report is not available at the time of the request, the type of incident, at minimum, should be included.

Of the 151 queries that did not have a proper case number documented, 92 (60%) of those queries were made from five employees/units. Two employees were combined to include one unit in this instance due to the employees working relationship on the squad. A reminder of the importance of proper documentation when making queries appears necessary to assist with compliance in this area of the ALPR program. A further breakdown of queries made during urgent times when a report number was not readily accessible was not performed, however, it should be understood these types of requests can occur and may not have a specific case number entered. During these types of situations enough information should be included to provide a clear case of law enforcement need.

Opportunities for improvement

1. ALPR administrators should do a better job of ensuring rosters are completed by attendees and these rosters are submitted for entry into ELM.
2. Active users who do not have documented training should be inactivated from the ALPR system until training can be verified or employees can be retrained with roster verification. Terminated/retired employees should be removed from the system.
3. Add volunteer trained employees to ELM to document ALPR training.
4. Work with the vendor to determine if mandatory audit entries (entry of GO or identification number) for all analytics is possible.
5. Due to the newness of the program, refresher training and/or reminders may be needed to ensure compliance to make sure users accompany data queries with case number of identification number information, when practical.